CLAIMS

[c1] 1. In a communication device, a method for providing security in a group communication network, the method comprising:

receiving an encryption key;

encrypting media for transmission to a controller using the received encryption key, the encrypted media being directed to another communication device; and

communicating the encrypted media to the controller, the communicating including wireless communication.

[c2] 2. The method of claim 1, wherein the receiving includes receiving the encryption key from a user of the communication device.

[c3] 3. The method of claim 1, wherein the receiving includes receiving the encryption key from a security module in the network.

[c4] 4. The method of claim 1, wherein the communication device is a push-to-talk (PTT) wireless communication device.

[c5] 5. In a communication device, a method for providing security in a group communication network, the method comprising:

receiving encrypted media from a controller; and

blocking the encrypted media if the communication device is not enabled to receive encrypted-media transmission.

[c6] 6. In a communication device, a method for providing security in a group communication network, the method comprising:

receiving encrypted media from a controller; and

blocking the encrypted media if the media is not encrypted based on an encryption key previously specified by the communication device.

[c7] 7. In a communication device, a computer-readable medium embodying a method for providing security in a group communication network, the method comprising:

receiving an encryption key;

encrypting media for transmission to a controller using the received encryption key, the encrypted media being directed to another communication device; and

communicating the encrypted media to the controller, the communicating including cellular communication.

[c8] 8. In a communication device, a computer-readable medium embodying a method for providing security in a group communication network, the method comprising:

receiving encrypted media from a controller; and

blocking the encrypted media if the communication device is not enabled to receive encrypted-media transmission.

[c9] 9. In a communication device, a computer-readable medium embodying a method for providing security in a group communication network, the method comprising:

receiving encrypted media from a controller; and

blocking the encrypted media if the media is not encrypted based on an encryption key previously specified by the communication device.

[c10] 10. A communication device for providing security in a group communication network, comprising:

means for receiving an encryption key;

means for encrypting media for transmission to a controller using the received encryption key, the encrypted media being directed to another communication device; and

means for communicating the encrypted media to the controller, the communicating including cellular communication.

[c11] 11. A communication device for providing security in a group communication network, comprising:

means for receiving encrypted media from a controller; and

means for blocking the encrypted media if the communication device is not enabled to receive encrypted-media transmission.

[c12] 12. A communication device for providing security in a group communication network, comprising:

means for receiving encrypted media from a controller; and

means for blocking the encrypted media if the media is not encrypted based on an encryption key previously specified by the communication device.

[c13] 13. A communication device for providing security in a group communication network, the communication device comprising:

a receiver to receive an encryption key;

a processor to encrypt media for transmission to a controller using the received encryption key, the processor being communicatively coupled to the receiver; and

a transmitter communicatively coupled to the processor to communicate the encrypted media to the controller, the communicating including wireless communication.

[c14] 14. The communication device of claim 13, wherein the communication device is a push-to-talk (PTT) cellular communication device.

[c15] 15. A communication device for providing security in a group communication network, the communication device comprising:

a receiver to receive encrypted media from a controller; and

a processor to block the encrypted media if the communication device is not enabled to receive encrypted-media transmission.

[c16] 16. The communication device of claim 15, wherein the communication device is a push-to-talk (PTT) device.

[c17] 17. A communication device for providing security in a group communication network, the communication device comprising:

a receiver to receive encrypted media from a controller; and

a processor to block the encrypted media if the media is not encrypted based on an encryption key previously specified by the communication device.

[c18] 18. The communication device of claim 17, wherein the communication device is a push-to-talk (PTT) device.

[c19] 19. A method for synchronizing encryption and decryption of a data frame in a communication network, the method comprising:

encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code;

encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code;

encrypting a second data frame based on a second unique code in the first communication device, said second unique code being derived from a second sequential code;

encapsulating said second encrypted data frame in a second transport frame, said second transport frame comprising a first portion and a second portion of said second sequential code; and

transmitting said first transport frame and said second transport frame to a second communication device,

wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code.

[c20] 20. The method of claim 19, wherein:

said first portion of said first sequential code and said first portion of said second sequential code each represent a short-term component of said first and second sequential codes, respectively; and

said second portion of said first sequential code and said second portion of said second sequential code each represent a long-term component of said first and second sequential codes, respectively.

[c21] 21. The method of claim 19 wherein said transport frame comprises a radio link protocol (RLP) frame.

[c22] 22. A method for synchronizing encryption and decryption of a data frame in a communication network, the method comprising:

receiving a first transport frame, said first transport frame comprising a first encrypted data payload, a first portion of a first sequential code, and a second portion of said first sequential code;

receiving a second transport frame, said second transport frame comprising a second encrypted data payload, a first portion of a second sequential code, and a second portion of said second sequential code; and

determining said second sequential code using said first portion of said second sequential code, said second portion of said second sequential code, and said second portion of said first sequential code,

wherein said first portion of said first sequential code and said first portion of said second sequential code identify the same relative portions of said first and second sequential codes, and said second portion of said second sequential code represents a successive relative portion with respect to said second portion of said first sequential code.

[c23] 23. The method of claim 22 further comprising:

decrypting said second encrypted data payload using said second sequential code.

[c24] 24. The method of claim 22 further comprising:

determining said first sequential code using said first portion of said first sequential code, said second portion of said first sequential code, and said second portion of said second sequential code.

[c25] 25. The method of claim 24 further comprising:

decrypting said first encrypted data payload using said first sequential code.

[c26] 26. A communication device for synchronizing encryption and decryption of a data frame in a group communication network, comprising:

a receiver to receive a data frame that is encrypted based on a unique code; and

a processor communicatively coupled to the receiver, the processor being capable of:

receiving successive portions of the unique code;

determining the unique code; and

decrypting the data frame based on the unique code.